Six Million (Suspected) Fake Stars in GitHub
A Growing Spiral of Popularity Contests, Spams, and Malware

Hao He   haohe@andrew.cmu.edu

Haoqin (Felix) Yang   haoqiny@andrew.cmu.edu

Philipp Burckhardt   philipp@socket.dev

Alexandros Kapravelos akaprav@ncsu.edu

Bogdan Vasilescu   vasilescu@cmu.edu
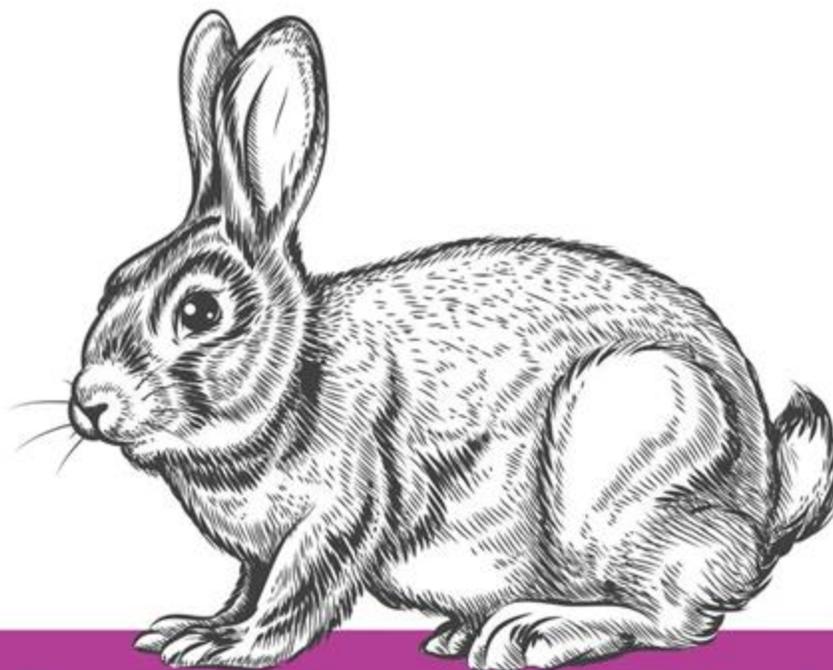
Christian Kästner   kaestner@cmu.edu

Motivation

Depending on a vague popularity contest

Choosing Based on GitHub Stars

You Only Live Once

O RLY?   @ThePracticalDev

Motivation

The more any **quantitative social indicator** is used for **social decision-making**…the more apt it will be to distort and corrupt the social processes it is intended to monitor.

– Donald T. Campbell, 1979

Motivation

The GitHub Black Market That Helps Coders Cheat the Popularity Contest

Popularity on GitHub can open valuable doors for developers and startups. Underground stores sell "stars" on the platform, offering coders a way to literally fake it till they make it.

https://www.wired.com/story/github-stars-black-market-coders-cheat/

Motivation

The GitHub Black Market That Helps Coders Cheat the Popularity Contest

KARI MCMAHON   BUSINESS   OCT 24, 2023 8:00 AM

Popularity on GitHub can open valuable doors for developers and startups. Underground stores sell "stars" on the platform, offering coders a way to literally fake it till they make it.

https://www.wired.com/story/github-stars-black-market-coders-cheat/

APPLICATION SECURITY   THREAT INTELLIGENCE   VULNERABILITIES & THREATS   CYBERATTACKS & DATA BF

'Stargazer Goblin' Amasses Rogue GitHub Accounts to Spread Malware

The threat group uses its "Stargazers Ghost Network" to star, fork, and watch malicious repos to make them seem legitimate, all to distribute a variety of notorious information-stealers-as-a-service.
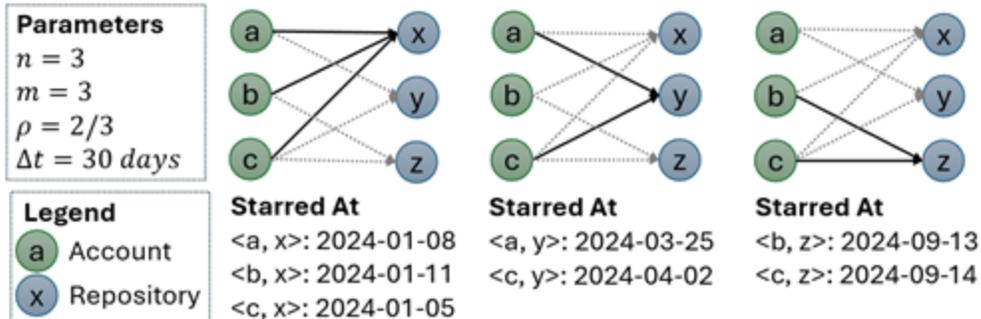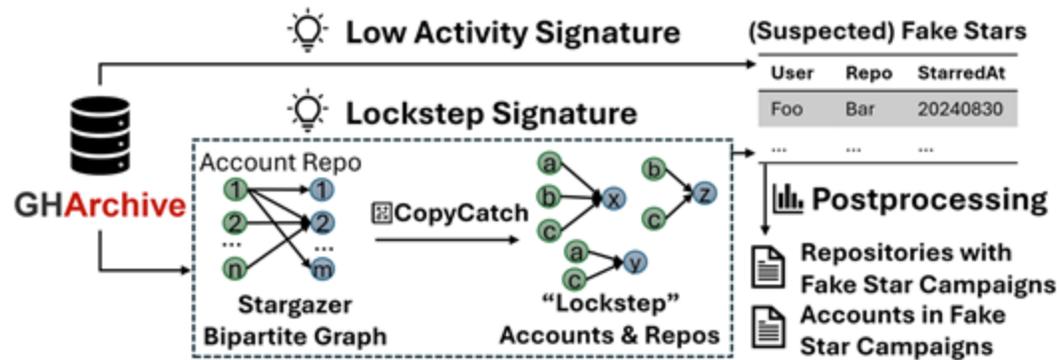
Jai Vijayan, Contributing Writer
July 24, 2024

4 Min Read

https://www.darkreading.com/application-security/stargazer-goblin-amasses-rogue-github-accounts-to-spread-malware

The Research Problems

- How bad is this problem?

- Are they really effective…
  - In popularity cheating?
  - In spreading malware?

- What can we do about it?

The GitHub Black Market That Helps Coders Cheat the Popularity Contest

KARI MCMAHON   BUSINESS   OCT 24. 2023 8:88 AM

Popularity on GitHub can open valuable doors for developers and startups. Underground stores sell "stars" on the platform, offering coders a way to literally fake it till they make it.

https://www.wired.com/story/github-stars-black-market-coders-cheat/

APPLICATION SECURITY   THREAT INTELLIGENCE   VULNERABILITIES & THREATS   CYBERATTACKS & DATA BF

'Stargazer Goblin' Amasses Rogue GitHub Accounts to Spread Malware

The threat group uses its "Stargazers Ghost Network" to star, fork, and watch malicious repos to make them seem legitimate, all to distribute a variety of notorious information-stealers-as-a-service.
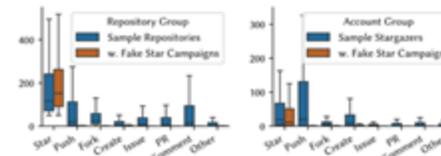
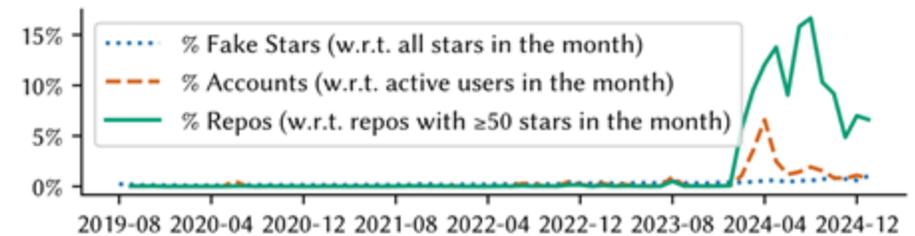Jai Vijayan, Contributing Writer
July 24, 2024

4 Min Read

https://www.darkreading.com/application-security/stargazer-goblin-amasses-rogue-github-accounts-to-spread-malware

Overview of Our Study

- StarScout - Detecting suspicious fake star activities at scale

- Measurement Study - Quantifying prevalence, domain, and impact

Measurement Study - Quantifying Prevalence, Domain, and Impact

Dataset

~6 million fake stars

18k repositories

301k accounts

- **Prevalence**

- **Patterns & Domain**

- **Promotional Impact**

- **Finding 1:** Fake star activities surged in 2024
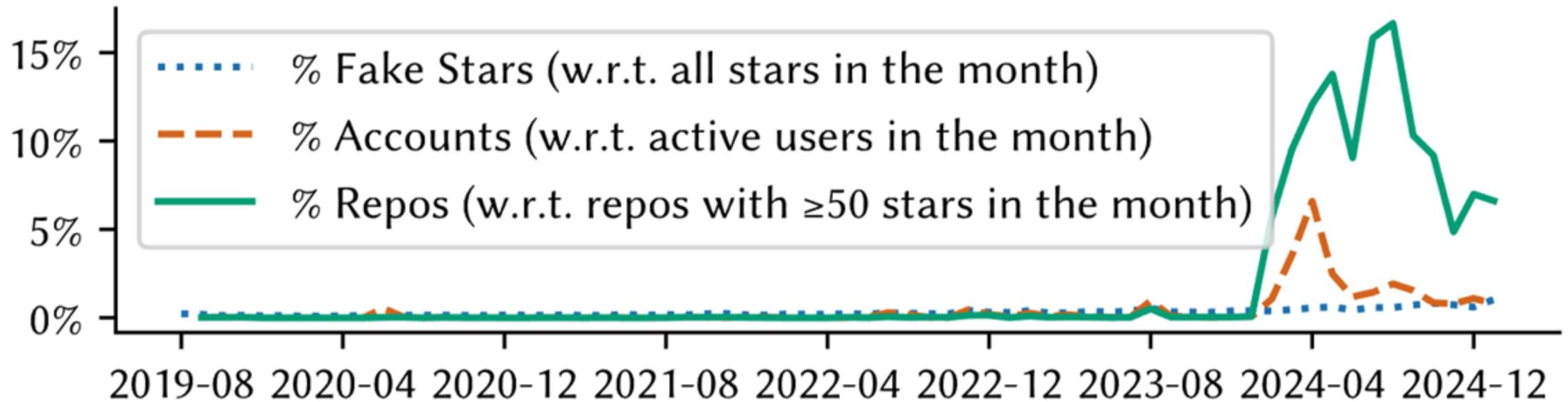
- **Finding 2:** Most repositories with fake star campaigns are short-lived, but accounts can stay active for a long time.
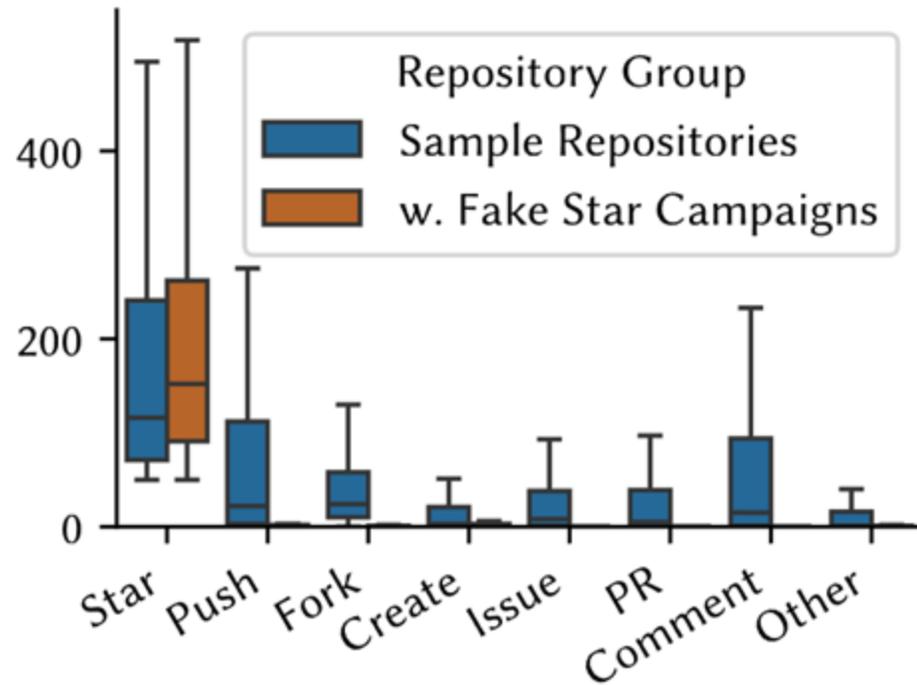
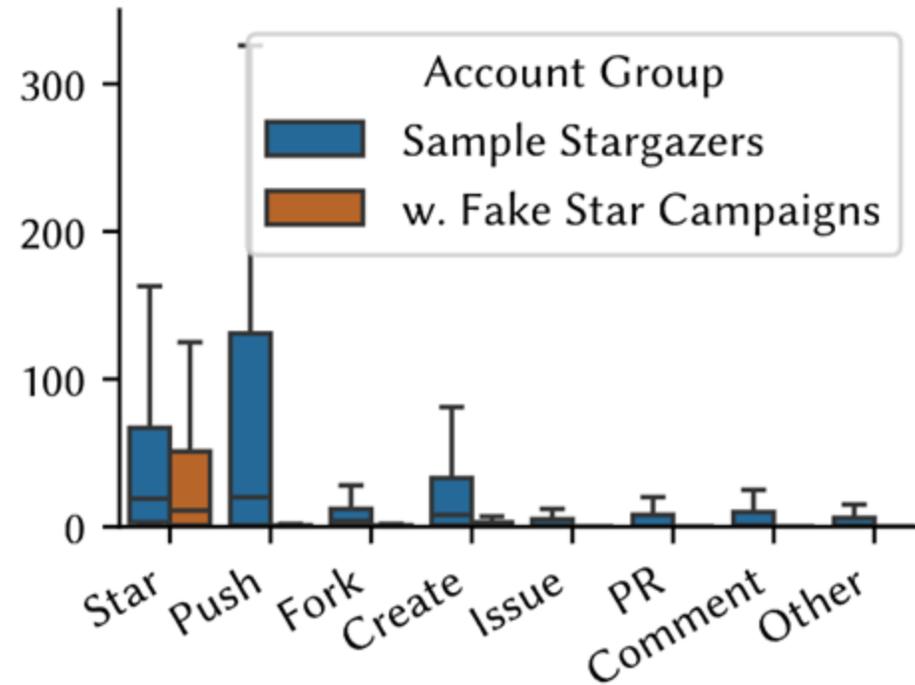Repository Lifespan

Median = 1 day

Account Lifespan

Median > 100 days

(Similar to regular accounts)

- **Finding 3:** Most fake star repositories and accounts do not have meaningful activities (e.g., issues, PRs, commits) beyond starring

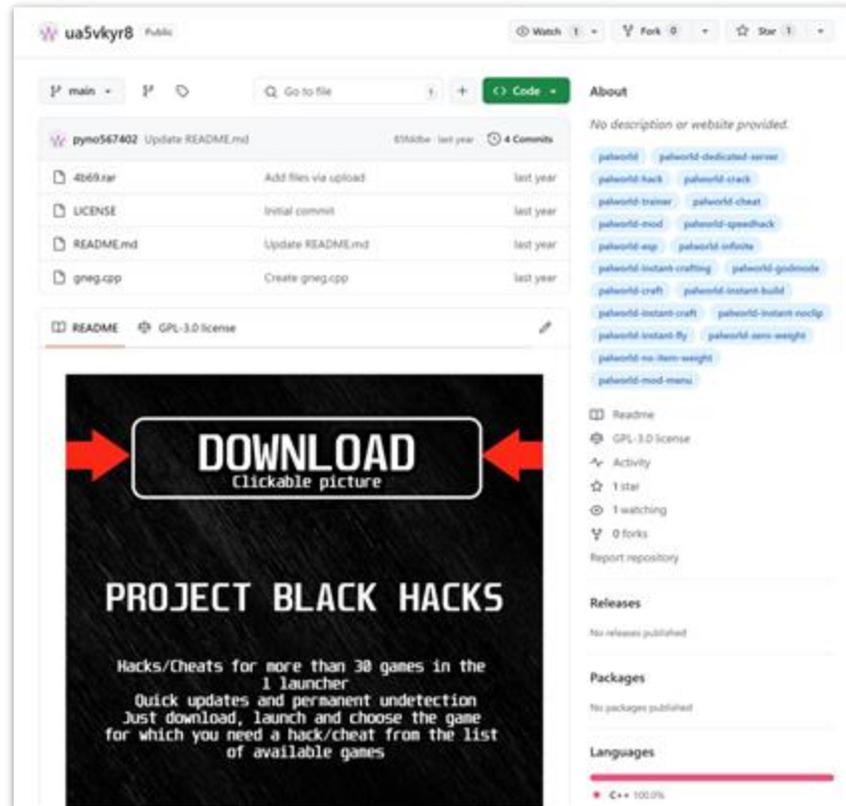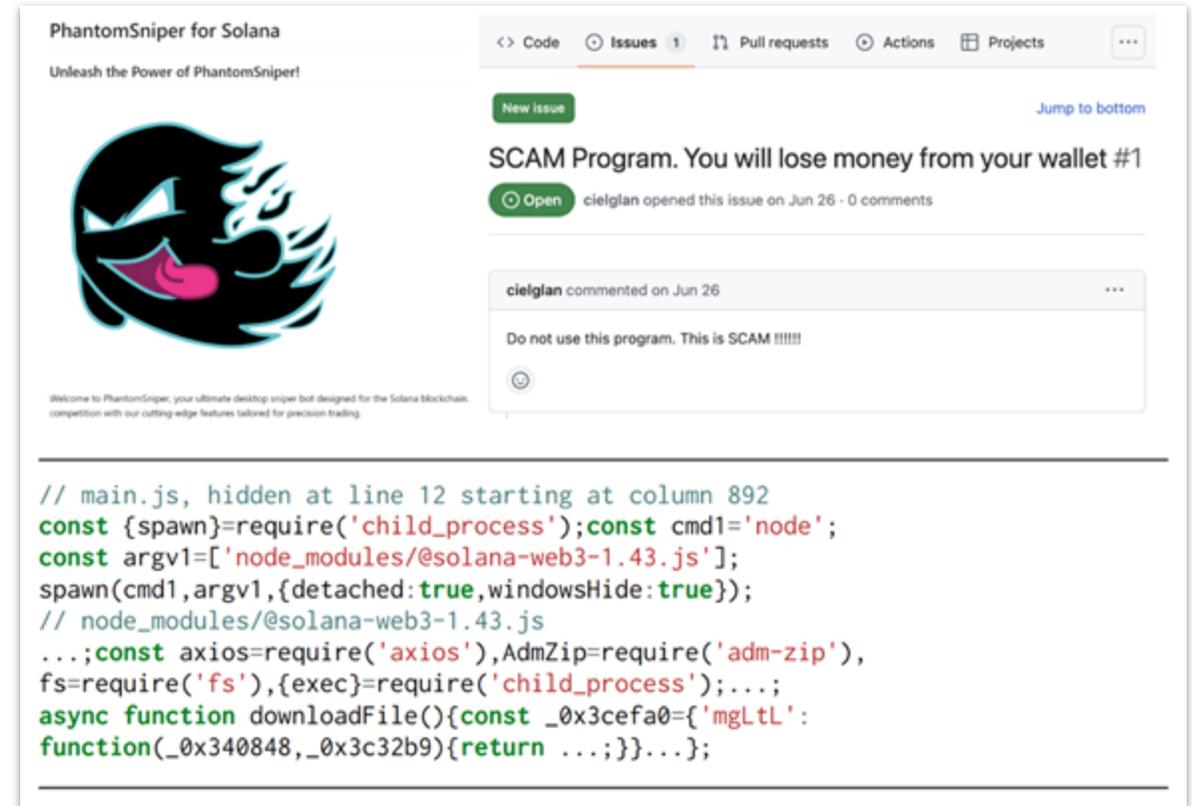a) Repositories

b) Accounts

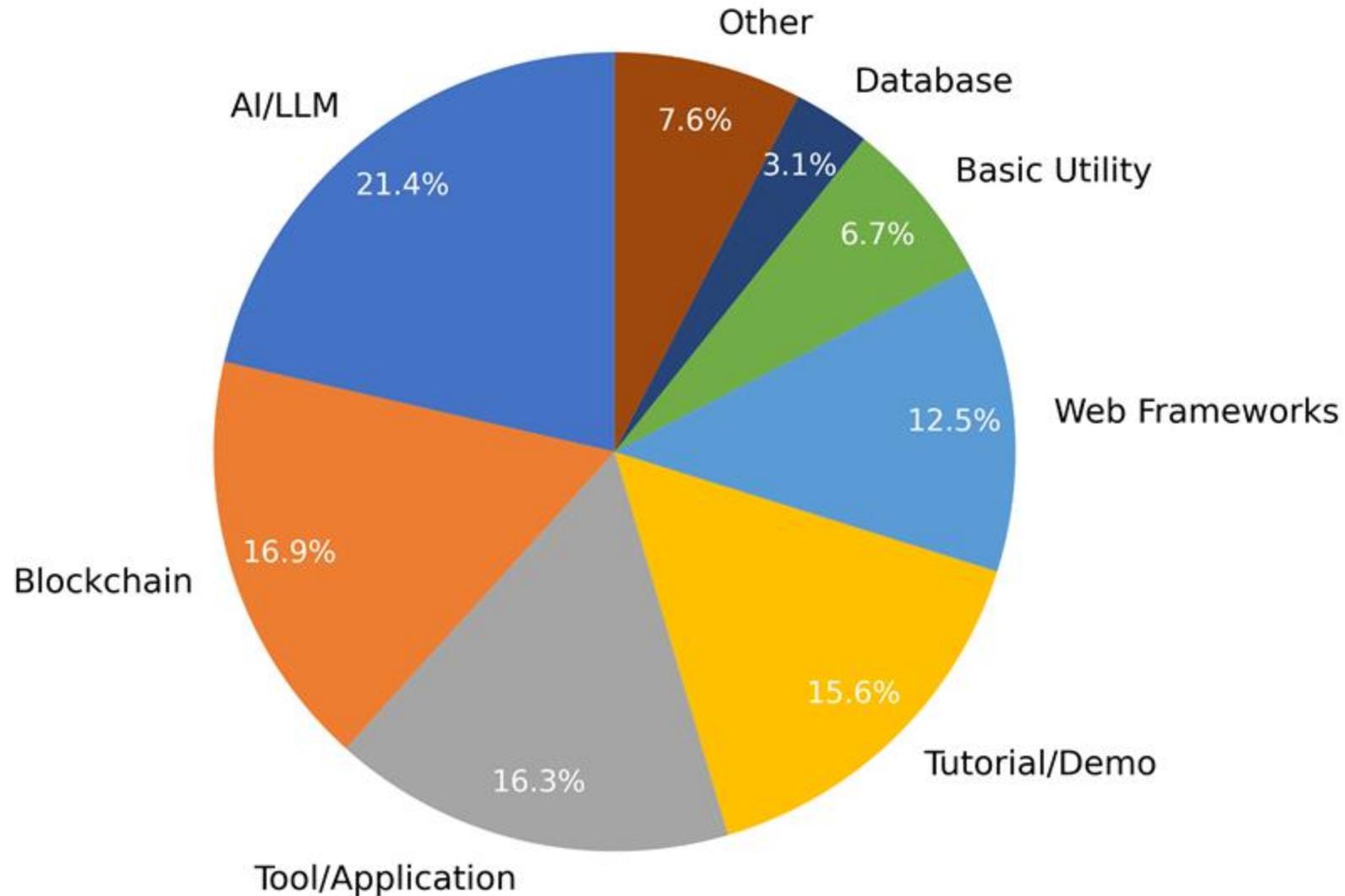- **Finding 4:** Most (~90%) of the fake star repositories are phishing malware

a) Example (game cheats)

b) Example (cryptocurrency)

- **Finding 5:** The remaining (~10%) include AI, crypto, app, tutorial, and web

- **Finding 6:** Fake stars bring a promotional impact in the short term but becomes a liability (leading to less real attention) in the long term

1% real star increase in month t

→ +**0.36% increase** since t + 1

→ +**0.15% increase** since t + 2

→ +**0.10% decrease** since t + 3
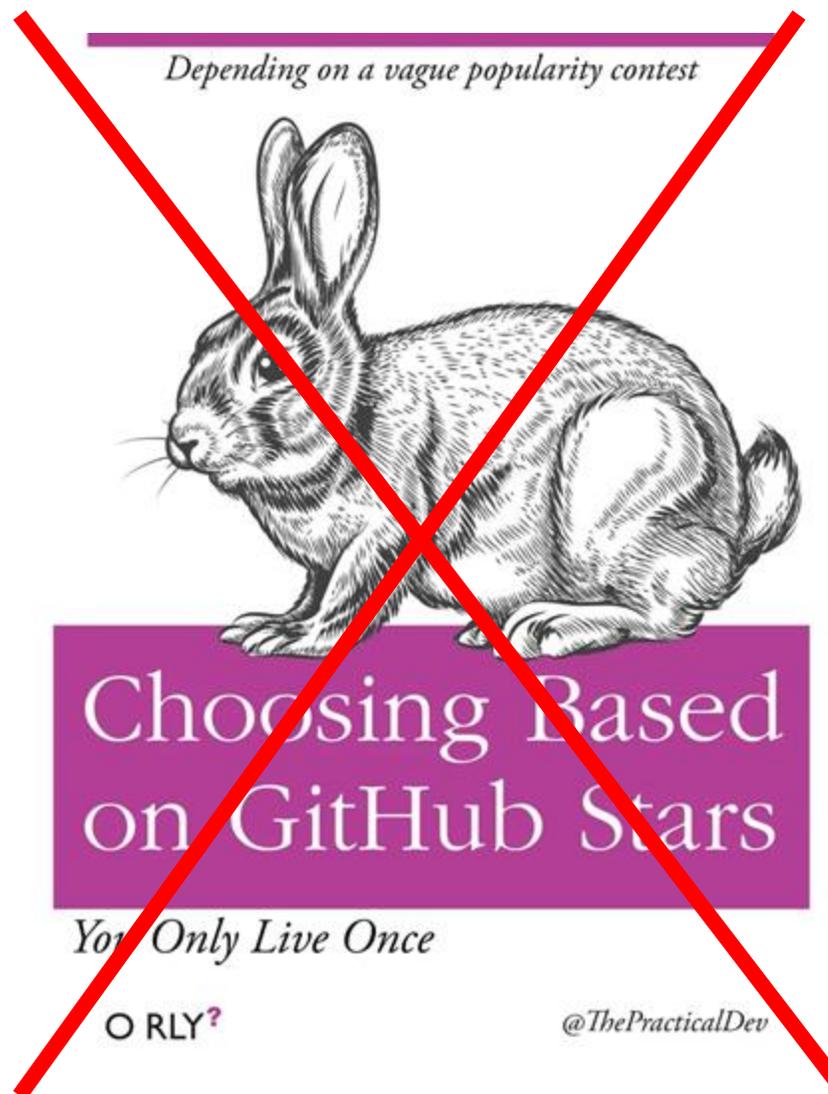
1% fake star increase in month t

→ +**0.07% increase** since t + 1

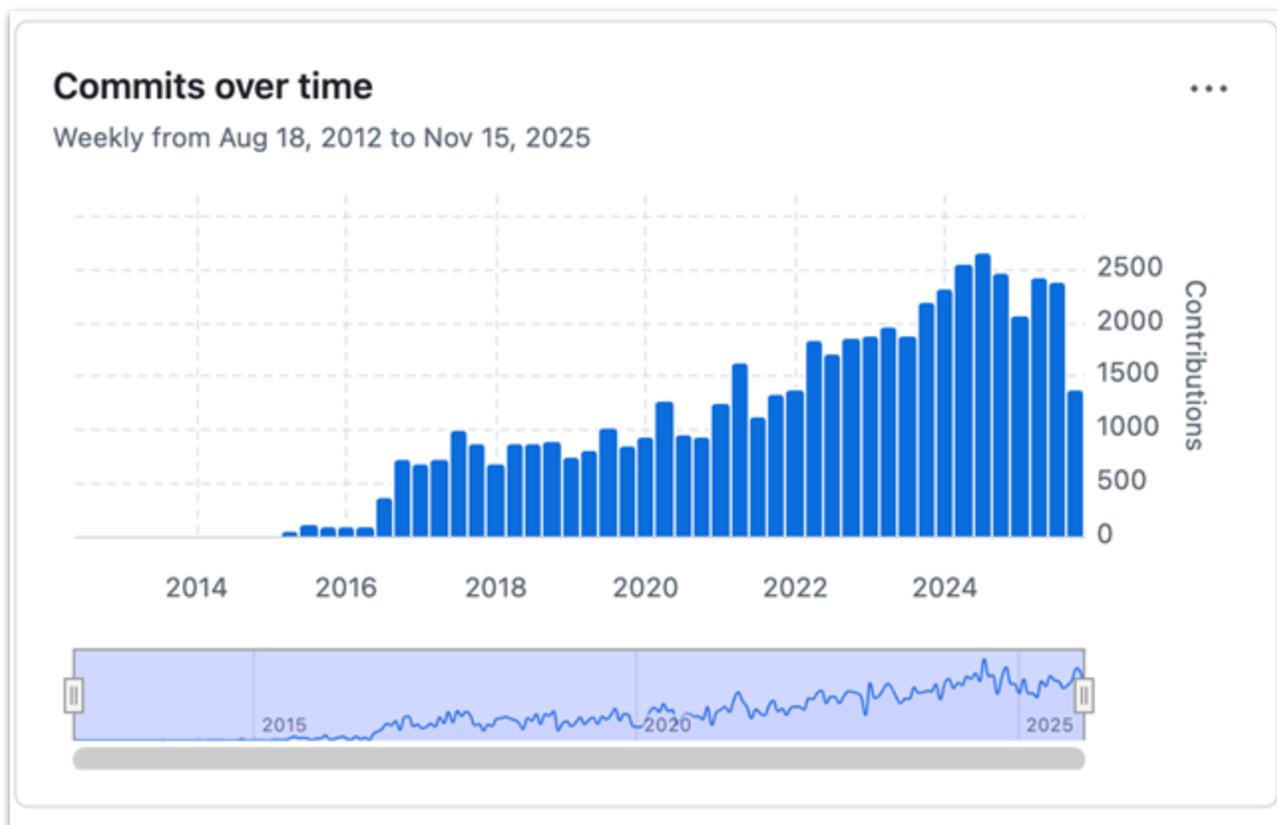→ +**0.03% increase** since t + 2

→ **-0.04% decrease** since t + 3

Takeaway 1: Star counts should **NOT** be used in high-stake decision scenarios

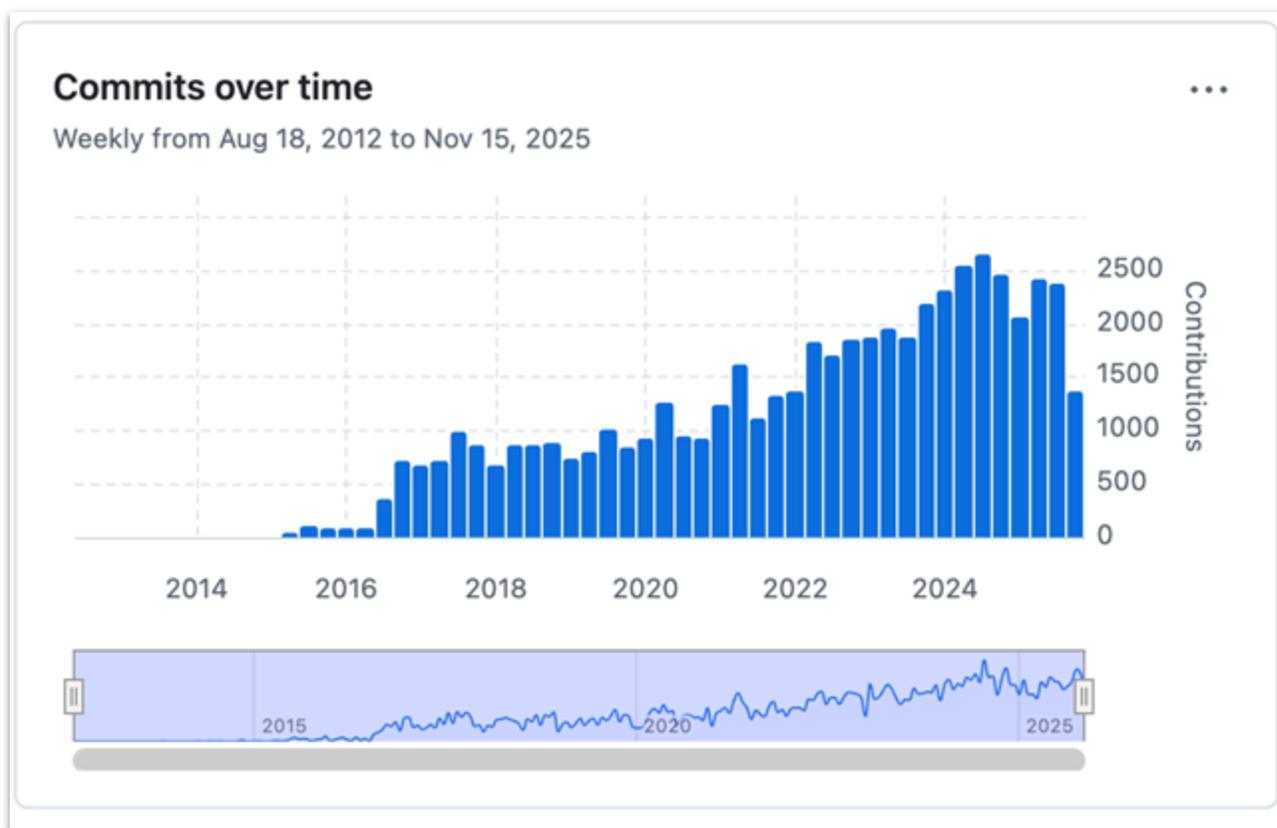# Takeaway 2: Activity, documentation, and community related signals matters

Commits over time
Weekly from Aug 18, 2012 to Nov 15, 2025

Community Standards

Here's how this project compares to recommended community standards.

Checklist

✓ Description

✓ README

✓ Code of conduct

✓ Contributing

✓ License

✓ Security policy

✓ Issue templates

✓ Pull request template

• Repository admins accept content reports

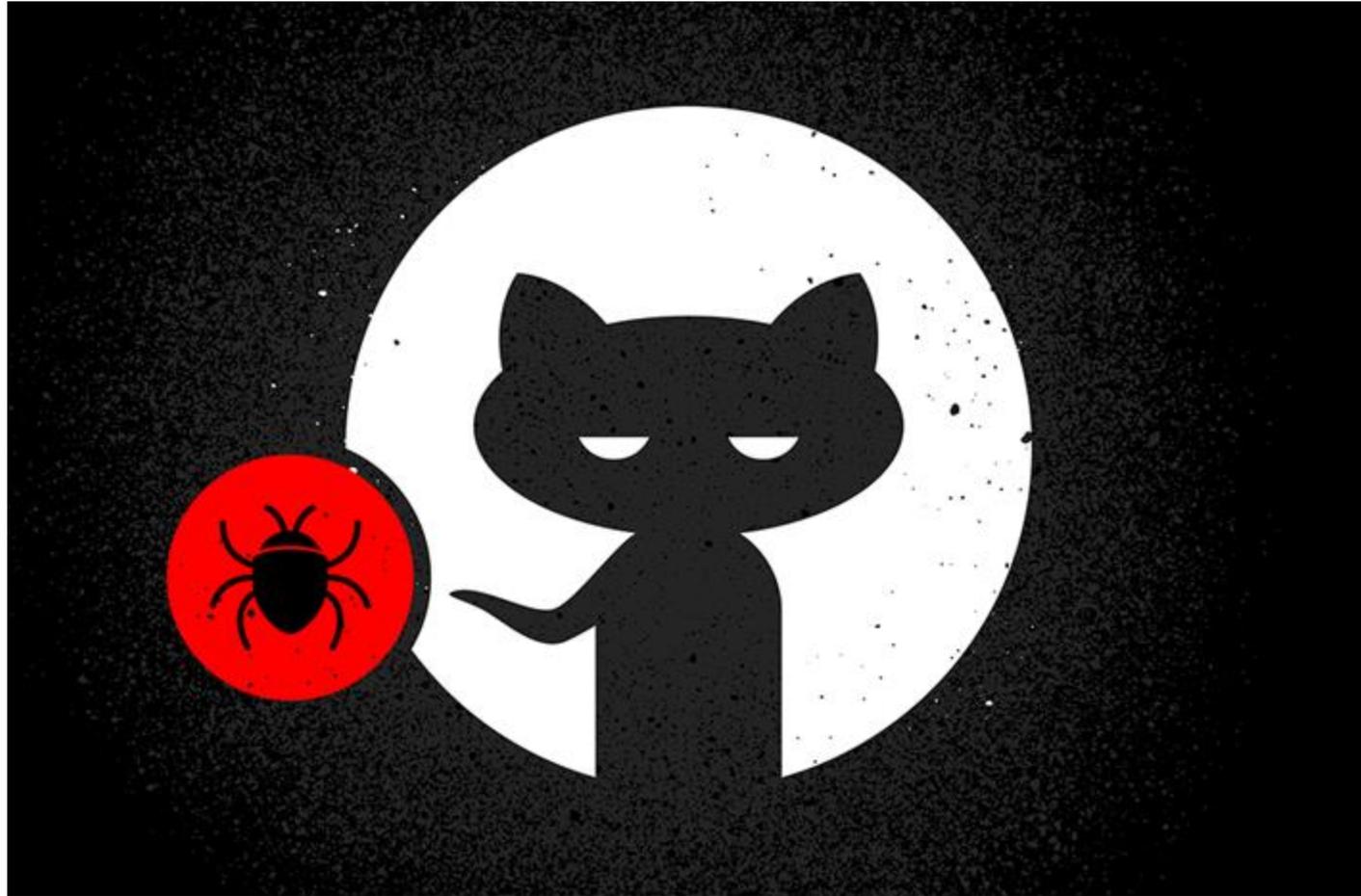# Takeaway 3: Community building matters more than artificial star count inflation

Takeaway 4: GitHub is becoming a popular attack target for malicious actors

Summary

- We have conducted the first large-scale measurement study on fake GitHub stars

- We have uncovered that:
  - Fake star activities surged in 2024
  - ~90% of fake stars are related to malicious activities, especially phishing
  - Remaining are on repositories in hyped domains (e.g., AI, crypto)
  - Fake stars are generally long-term liability with no meaningful promotion impact

Download Paper

Summary

- We have conducted the first large-scale measurement study on fake GitHub stars

- We have uncovered that:
  - Fake star activities surged in 2024
  - ~90% of fake stars are related to malicious activities, especially phishing
  - Remaining are on repositories in hyped domains (e.g., AI, crypto)
  - Fake stars are generally long-term liability with no meaningful promotion impact

Download Paper